# NETWORKS: ADAPTING TO UNCERTAINTY

By Henry S. Kenyon

Communications are vital to coordinating U.S. military operations. Formed into networks, wired and wireless equipment pass voice, video, and other data between far-flung battlefields and headquarters facilities in North America. Advanced weapons and sensor systems also communicate with each other and with warfighters to convey time-critical information about fleeting enemy targets, a key tenet of network-centric warfare.

However, these networks are also vulnerable to jamming and other types of interference. Remote sensors and guided weapons must be able to function and coordinate themselves when disconnected from a network and the networks themselves must be able to repair and reconnect themselves as nodes are lost or acquired during fluid military operations.

DARPA is involved in several initiatives designed to provide U.S. warfighters with robust, self-forming, and self-defending networks at the strategic and tactical levels. The agency's Strategic Technology Office (STO) has been at the forefront of this development.

According to David Honey, who recently stepped down as STO director, the office's initial foray into mobile, ad-hoc self-forming networks was in the Small Unit Operations-Situational Awareness System (SUO-SAS) program. Launched in the late 1990s, this program was the first attempt to determine if such networks could exist, support military applications, and work in an operational environment. Experiences in previous conflicts supported the need for a robust communications system for small units. "For tactical military operations, you cannot rely upon having access to a fixed infrastructure," he said.

When DARPA launched the initiative, Honey said, the U.S. Department of Defense (DoD) and its contractor community knew how to build radios, but it was uncertain if a real network radio could be made to enable network-centric warfare activities. "The idea with SUO-SAS was that it would truly be a self-forming, self-managing, self-healing network for soldier-level radio communications," he said.

At that time, it was considered doubtful that a man-portable system could demonstrate such robust capability in a mobile, ad-hoc networking environment. The first prototype radios constructed to host the SUO-SAS software application were large and bulky. Honey stated that the technology demonstration models weighed more than 40 pounds. These early technology demonstration prototypes were not optimized for size, weight, and power, but rather created out of commercially available radio parts just to validate that robust mobile networking was feasible.

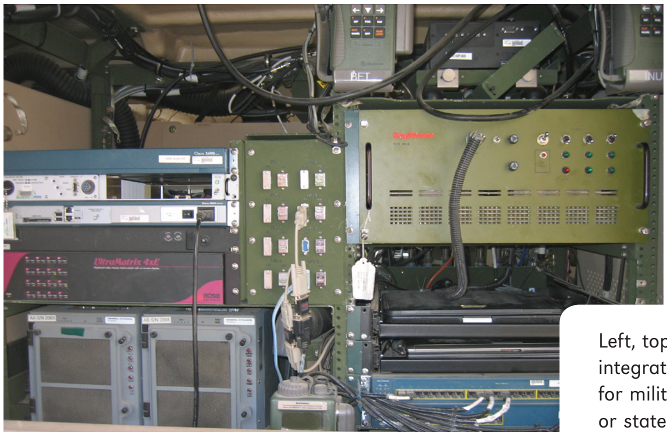
The heart of the system was its software. A soldier could pick the radio up, turn it on, and the software and equipment would acquire the correct channel. "That's the last thing that they [the radios] would do with any human in the loop as far as that network was concerned. The radios would be able to reach out, find each other, and form local area networks. Potentially, they would use a bridge to go from one local area network to another," he explained.

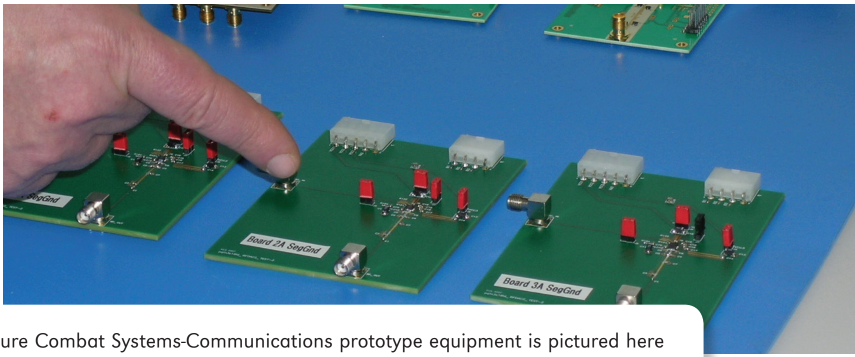
The radios also could utilize radio nodes on airborne platforms to provide beyond-line-of-sight communications. In other words, the network was intelligent enough to recognize the similar radio, admit it to the network, and use it as a relay point. But to prevent an unintentional denial of service attack, only one radio in the local dismounted network was allowed to communicate through the new node. However, messaging and data were instead dynamically distributed across the network to avoid any single point of failure.

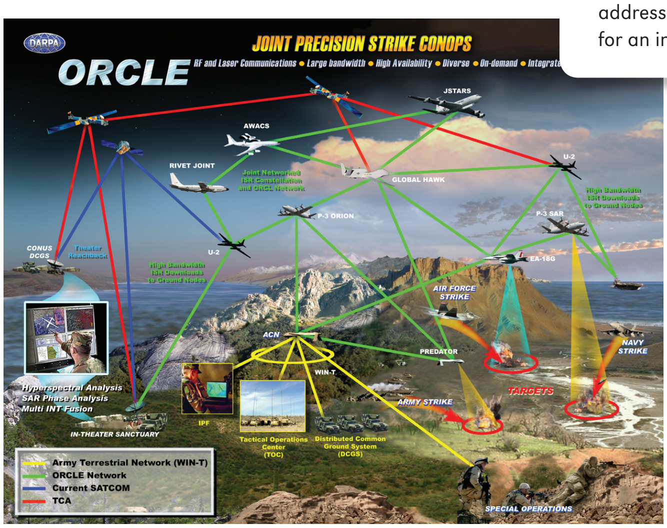
The Small Unit Operations-Situational Awareness System, pictured above, marked DARPA's initial research into whether mobile, ad-hoc self-forming networks could exist.

Image courtesy of DARPA

Another important feature of the SUO-SAS network was its ability to self-heal. If a soldier went into a cave or a building and dropped out of the network, the system would reroute traffic around the break. When the soldier re-emerged into an area where radio transmissions could be received, the network would recognize the node and automatically readmit it without any intervention by the user. "The SUO-SAS program was the first really big push into self-forming radio networks, and it worked very well," said Honey. The DARPA program concluded in 2002.






DARPA
JOINT PRECISION STRIKE CONOPS
ORCLE
RF and Laser Communications • Large bandwidth • High Availability • Diverse • On-demand • Integrate
JSTARS
AWACS
RIVET JOINT
Joint Networked ISR Constellation and ORCL Network
GLOBAL HAWK
U-2
High Bandwidth ISR Downloads to Ground Nodes
P-3 ORION
P-3 SAR
CONUS DCGS
Theater Reachback
U-2
High Bandwidth ISR Downloads to Ground Nodes
EA-18G
AIR FORCE STRIKE
NAVY STRIKE
ACN
PREDATOR
WIN-T
TARGETS
ARMY STRIKE
Hyperspectral Analysis
SAR Phase Analysis
Multi INT Fusion
IN-THEATER SANCTUARY
IPF
Tactical Operations Center (TOC)
Distributed Common Ground System (DCGS)
Army Terrestrial Network (WIN-T)
ORCLE Network
Current SATCOM
TCA
SPECIAL OPERATIONS

Left, top: Future Combat Systems-Communications prototype equipment is pictured here integrated with a full Gateway and satellite system. This equipment makes it possible for military personnel to maintain lines of communication, regardless of field conditions or state of hardware. Left, bottom: An ORCLE graphic depicts how communications via optical laser links would work. Above: DARPA's Wireless Networks after Next program addresses communications on the individual level; the circuits pictured here form the basis for an inexpensive, four-channel radio being developed by DARPA.

From this first success, the military adopted several SUO-SAS-based technologies. DARPA transitioned the radio portion to the U.S. Army Communications Engineering Research, Development and Engineering Center for further technology maturation and development. The result was a hand-held version of the SUO-SAS radio, called Soldier Radio, and the Joint Program Executive Officer, Joint Tactical Radio System (JTRS), adopting the SUO-SAS waveform for its family of JTRS radios. Honey added that a common characteristic of all of DARPA's self-forming radio programs is field experimentation by soldiers, which is a crucial part of evaluating military utility for this network-centric warfare system. "It all worked out very, very well," he said.

## THE STATE OF THE ART

The SUO-SAS man-portable radios were based on an omni-directional antenna system to support communications between small groups of soldiers. However, new, more ambitious programs required different capabilities; for example, better spectrum efficiency and higher data rate.

The U.S. Army's Future Combat Systems (FCS) program was initiated to transform the Army into a more responsive and agile maneuver force. Because the proposed vehicles were much smaller than Abrams tanks, new ways for improving survivability other than steel, while preserving lethality, were required. This was accomplished by restructuring platoons and companies around a family of networked vehicles and weapons systems to provide survivability and lethal response like a Navy Carrier Strike Group. FCS was built on the idea that networks can form the basis for field operations such as fire support and other tools to aid warfighters in combat operations. The new network, called FCS Communications (FCS-C), needed high-bandwidth data rates between the various nodes and robust low probability of detection/intercept. In addition, as the Army's operational requirements grew, the network itself began to evolve into a more sophisticated and robust platform.

The DARPA FCS-C program featured new capabilities, such as directional antennas built into the system to reuse and optimize available spectrum. Honey explained that the ability to switch spectrum bands is vital because, depending on field conditions, the network itself could choose its optimal operating frequency. This capability necessitated that quality of service become an important aspect of the program. He described quality of service as a radio frequency (RF) self-managing network's ability to support sophisticated applications that warfighters would want to access during combat operations.

Another important part of the FCS-C effort is the FCS-C Gateway program. By upgrading the FCS-C network to operate as a gateway rather than a router system, DARPA demonstrated that previously incompatible tactical radios can communicate seamlessly by using the network's Internet protocol layer. This method offers the potential for more affordable military communications between legacy and coalition radios in the future. The FCS-C Gateway system has transitioned to the U.S. Special Operations Command for evaluation and use.

As the FCS-C program matured and demonstrated these capabilities, the research into the technology's leading edge began moving toward two opposite ends of the networked spectrum, Honey noted. One program goal was the need to install a high-throughput network in a theater of operations that could also tie into the Global Information Grid without being dependent on satellite links. To meet

Images courtesy of DARPA

this requirement, DARPA launched the Optical RF Combined Link Experiment (ORCLE) program, now known as Optical RF Communications Adjunct (ORCA). ORCLE and its successor program are based on the idea that U.S. forces will use free-space, optical laser links between moving platforms with no need for humans to establish the connections, with RF providing high-priority communications when cloud conditions appear. These links will manage themselves in a self-healing network that will reroute data around any obstructions.

Information will be seamlessly handed off to an RF link that coexists with the optical link. This capability will provide an in-theater high-data transport system that also serves as a backbone, Honey explained. The backbone will permit laser terminals to serve as fiber-optic points of presence. He noted that this system will allow warfighters to use the high-bandwidth, tactical-laser link to immediately contact intelligence centers in the continental United States without being dependent on satellite communications.

The other end of the program's spectrum focuses on individual warfighters. This important networking technology area is the focus of DARPA's Wireless Networks after Next (WNaN) program. This effort intends to provide every soldier with a $500 dollar, four-channel radio. This radio will be inexpensive and will feature some of the major technology efforts that DARPA has developed over the last several years.

For example, the goal of the Next Generation (XG) radio program – one of WNaN's sub-programs – is to permit radios to opportunistically network with each other. "Not just point-to-point links, but entire networks of radios existing and operating in unused parts of the spectrum without causing interference to legitimate users of those frequencies or to non-XG systems," said Honey. This XG networking capability will be built into WNaN equipment.

The system will also feature disruption-tolerant networking. Honey noted that link disruptions are an unfortunate fact of current mobile tactical communications. A major cause of these disruptions is due to the software architecture of transmission protocol/Internet protocol (TCP/IP) messaging. When a TCP/IP-based message is interrupted, it automatically restarts the data transmission. DARPA is developing fault-tolerant networking technologies that can take advantage of existing memory throughout the network, store information locally, and allow a session to restart where it stopped. "It makes the network responsible for getting the data to the endpoint, rather than the two endpoints themselves having a live connection in order to do that. The [WNaN] soldier radio will feature this capability," he said.

## UNATTENDED SYSTEMS

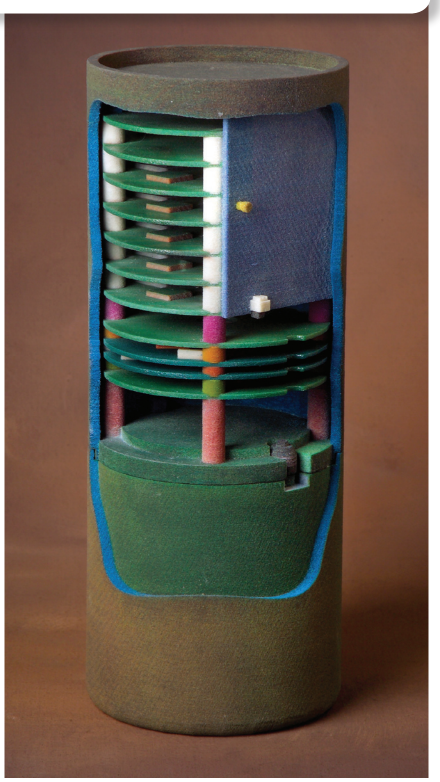
Honey noted that a major difference between the wired and wireless domains is that wired environments enjoy ample bandwidth and unlimited energy to power devices and applications. "The boxes in the wired domain plug into a wall socket, and that's the last you really have worry about it [power]," he said. But many wireless systems, especially the hand-held devices soldiers rely on, depend on batteries. Batteries have limited lifetimes that shorten every time a bit of data is transmitted, he said.

Battery-powered wireless systems cannot waste energy by periodically sending out status information like nodes in wired networks do to maintain routing tables. "If you send that kind of stuff out in the wired domain, it's not a problem, it's a help. In the wireless domain, if you have an unattended ground sensor [UGS] network and every node keeps sending out all these keep-alive packets, those batteries will eventually deplete. If soldiers have to go out at great risk to emplace those nodes out in the field, to have them go out to change the batteries could be a problem," Honey said.

Depending on how the military decides to use UGS networks, Honey believes that rewriting the devices' software protocol stack and modifying their RF front ends for increased energy efficiency is an opportunity for warfighters. He explained that the UGS will be the dismounted soldier's greatest aid in future conflicts because the devices can serve as sentries to monitor the environment and warn of enemy activity without troops being physically present.

To help achieve these networked warfighting goals, DARPA's Connectionless Networks program has developed technologies for a new generation of UGS devices. The effort worked to achieve greater efficiency, more battery life, and better design of the devices' RF front ends to specifically operate in a wireless environment.

Another DARPA program that pushed forward the possibilities of wireless networks and systems was the Wolfpack program. A key part of Wolfpack was the need to form robust, self-forming networks to aid soldiers in the field. The goal of the effort was to create a family of deployable remote devices that could sense a range of enemy communications and selectively jam them, with every remote node in an area contributing to intercepting the transmission. Honey noted that the first production units of this technology became available to warfighters early last year. "It's a great tool that will use all of those aspects of self-forming networks to deliver for the soldier the ability to monitor adversary RF traffic," he said.



A Wolfpack production unit. Warfighters can use this technology to selectively jam enemy communications.

Photo courtesy of DARPA

## CHALLENGES AND FUTURE REQUIREMENTS

As these new wireless capabilities are developed, Honey believes that the next set of challenges will be creating the applications, tactics, techniques, and procedures to use these systems effectively. He explained that, like any tool, there will need to be a substantial amount of experimentation to determine the best methods to use these devices.

The future challenge facing the DoD is that the electromagnetic environment is becoming very dense. Honey explained that the amount of commercial and military signals will grow enormously and this crowding will require the military to develop hardware that can operate in a bandwidth-constrained environment. He added that DARPA's Microsystems Technology Office is working on developing component-level technologies that will allow the military to have these future, flexible radio systems.

Besides warfighters, another group facing a complex radio communications environment consists of first-responders, fire, and law enforcement emergency personnel. Like the military, first-responders all must work with legacy systems that cannot be replaced overnight. In fact, Honey admitted that interoperability remains a major challenge for network-centric warfare. He noted that there are two schools of thought about overcoming this impediment. The first approach is to use radios that can communicate with all other types of radios. The drawback to this method is that these new radios must be widely purchased, which can become very expensive for state and local agencies.

The other approach recognizes that multiple organizations will not all have the same equipment. In the case of the DoD, there will be units that cannot afford to upgrade in a timely fashion or coalition forces who arrive at an operation with different radios. In the first-responder market, the question of legacy equipment will remain open for the foreseeable future. "Everybody can't upgrade to a particular radio at a particular point in time. So integrating legacy [equipment] will be a challenge for a while," said Honey.

A third dimension to the interoperability issue is the need for the DoD to operate in a first-responder mode in another nation, such as supporting relief operations in the aftermath of a tsunami-type disaster. Honey observed that this sort of international disaster recovery operation puts military forces in communication with a variety of nongovernmental organizations and other governments, all of whom are using different radios. "How do you cope with that?" he asked.

To meet communications needs in a multinational, legacy environment, DARPA developed the concept of making the network responsible for translating and interoperability functions by hosting these services. Known as a gateway approach, Honey noted that it is widely used in commercial communications' services. For example, gateways allow people with different cell phones to communicate because the translation and interoperability function resides in the gateway itself.

However, Honey explained that current gateways have some difficulty with translation and interoperability because they use TCP/IP-based as opposed to fully mobile ad-hoc network (MANET)-based systems. DARPA recently solved this challenge by developing, deploying, and field-testing true MANET-based gateways. He says that these gateways demonstrated that analog and digital radios can interoperate and communicate via the network with a properly configured MANET gateway.

For first-responders, the DoD, and government agencies that may have to respond to civilian humanitarian crises in other countries, the ability to deploy a MANET gateway will allow them to put interoperability and translation capabilities directly into the network. Once this MANET-based capability is available, another challenge will be determining the application-level opportunities to allow different civilian and government groups to work effectively together. Honey explained that this is analogous to the early days of the Internet, when the connectivity was available, but e-mail, Web browsing, and other types of distributed collaboration tools taken for granted today were unavailable. "I think that there's a huge opportunity for people to develop new capabilities in that particular application space," he said.